

ENCRYPTO

I. Project Notes

A. Definition of Terms

- Encryption - to alter (a file, for example) using a secret code so as to be unintelligible to unauthorized parties.
- Cryptography - The process or skill of communicating in or deciphering secret writings or ciphers.
- Plain text – also called as clear text; a message readable by humans.
- Cipher text - A message obscured by applying an encryption algorithm.
- Encrypt - The process by which plain text is converted into cipher text.
- Decrypt - The process of converting cipher text into plain text.
- Key - The formula used to decrypt an encrypted message.

B. Introduction

Encryption is not an invention of the 21st Century. In fact, the ancient civilizations already utilized the use of encryption in concealing their plain text messages as early as 4000B.C. The scribes of Egypt used cryptography to preserve the secrecy of their religious rituals. The Spartans used a device known as the Scytale to pass on secret messages while they were at war. Finally, the Germans had the Enigma machine that helped them conceal their messages with each other during the World War II.

The primary reason for encrypting plain text is for privacy and security. With today's technology, we just not prevent thieves from stealing our money, but also, we protect our identity from getting stolen. Data encryption plays a major role in ensuring customers that their activities thru a network are secure.

The rationale behind our project is to provide users an application in which they could use to communicate with each other without sacrificing their privacy. We created a peer-to-peer chat application with a special feature to encrypt and decrypt messages before and after sending them thru a network.

C. Other possible C++ Projects:

1. Calendar

This is an application similar to a yahoo calendar which the user could easily update.

2. Sticky Notes

An application that is typically displayed on the user's desktop. The application is an equivalent of the old fashioned post it, in which users place their things-to-do list.

3. File encrypting application

An application that could easily convert any document (regardless of file type) to a non-readable format.

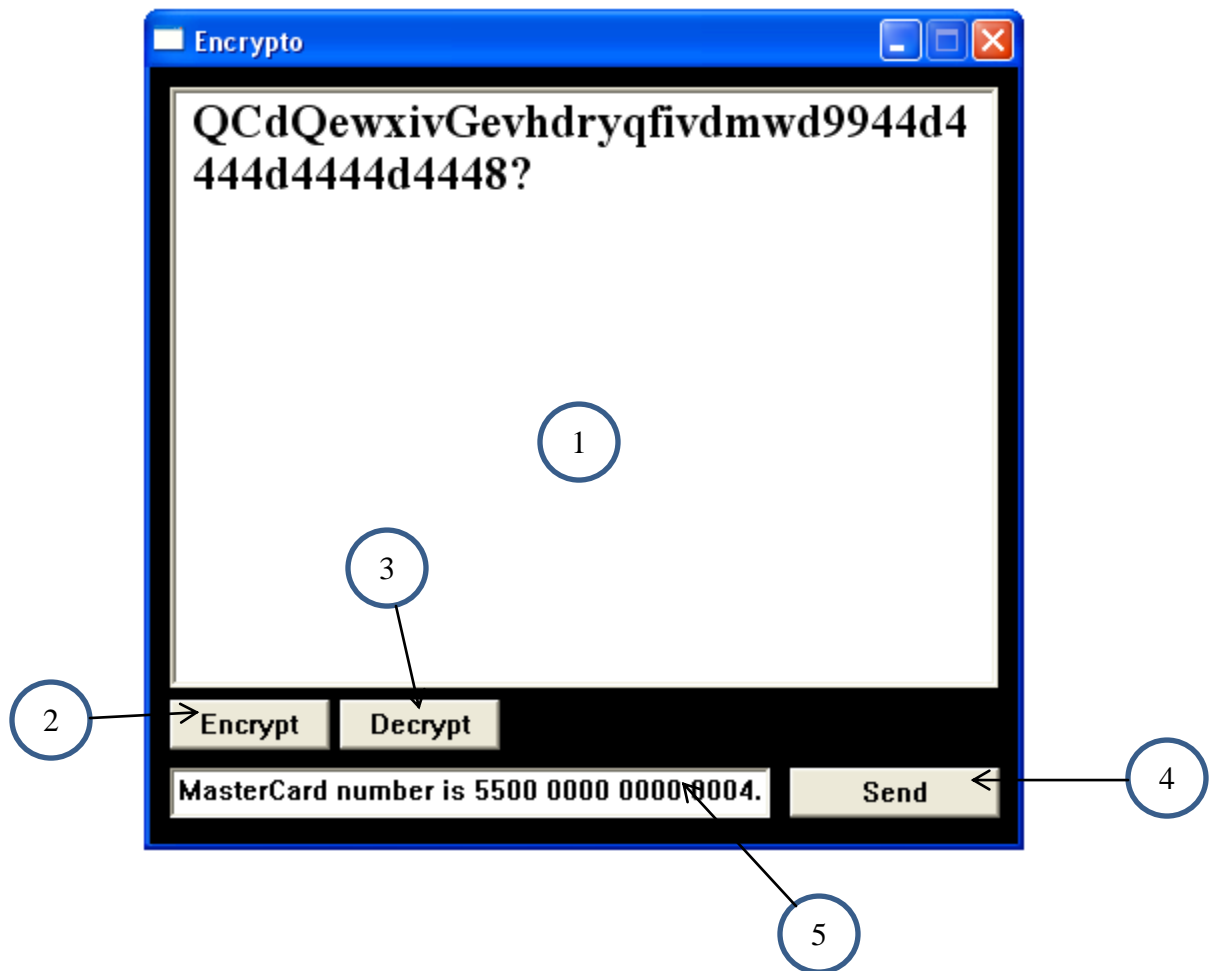
D. The Developers

- Clark Jason Cacal
- John Finly Dacanay
- Michael John Servano

II. Project Design

A. GUI

Overview of the GUI



1. Display Textbox
2. Encrypt Button
3. Decrypt Button
4. Send Button
5. Message Textbox

GUI commands

1. Set server port

– [[openport<space><port number>

2. Set destination address and port

– [[connect<space><port number><space><IP address>

3. Set encryption/ decryption key

– [[setkey<space><keystring>

Note:

1. The port number for computer's 1 and 2 should be the same.
2. The IP address entry should be the IP address of your peer.
3. The key entered should be the same.

B. Encryption

Encryption (Private key)

Private key encryption involves the use of a key known only to the users of the application. This secret key is used when encrypting or decrypting the messages.

Encryption Algorithm

ENCRYPTO utilizes the use of an improved version of the Caesar's algorithm. In the Caesar's algorithm, each letter in the plain text is replaced by a letter some fixed number of positions down the fixed array of characters.

Example:

Plain: abcdefghijklmnopqrstuvwxyz
Cipher: defghijklmnopqrstuvwxyzabc

In this example, each letter in the plain text is substituted by the letter three characters away.

Our modification involves the use of the concept of key and the use of the ASCII table in conjunction with how the Caesar's algorithm works. First, we convert the entered key by the user to a decimal number. For example, "dot" is the key entered by the user. We convert each letter by the corresponding decimal value then add the total of all the numbers.

d = 100

o = 111

t = 116

sum = 327

Second step is we use the modulo operator to the sum and the total number of characters we are using. Assuming, we are using only the small letters of the English alphabet which involves 26 characters, we use 26 as our 2nd number.

Applying, we have,

$327 \% 26 = 15$

The resulting number would be the number of shifts our original array of characters would make. If we are using only the small letters of the English alphabet, a becomes p, b becomes q and so on. In the ENCRYPTO application, we used a total of 95 characters. This means that we would apply the modulo operator with the sum of the letters of the key and with 95. After that we would apply the number of shift through our array of 95 characters.

C. Networking

ENCRYPTO can only be used by two work stations at a time. The GUI command lines described at the GUI section are entered so that the two computers could connect to each other.

D. System Requirements

ENCRYPTO will run on any 32-bit Windows Machine and up.

Sources:

Basic concepts of encryption. <http://library.thinkquest.org/27158/concept.html>

Use of data encryption in today's context: e-commerce
<http://library.thinkquest.org/27158/concept.html>

Vine, M. (2008). *C programming for the absolute beginners*. Boston: Thomson Course Technology.

Caesar's algorithm. http://en.wikipedia.org/wiki/Caesar_cipher